In the Claims:

1. (Currently amended) A method for ~~securely storing~~ hiding information on a computer, [[said]] the method comprising ~~the steps of~~:

a) retrieving an identity of ~~at least one~~ a computer component;

b) deriving ~~at least one identifier~~ a name from said identity in a secret manner ~~of said at least one computer component~~; and

c) ~~for each of said at least one identifier,~~ storing [[said]] the information on [[said]] the computer in a storage entry ~~corresponding to~~ identified by said ~~identifier~~ name.

2. (Canceled)

3. (Currently amended) [[A]] The method according to claim 1, wherein [[said]] the information is encrypted prior to said storing ~~of said information~~.

4. (Currently amended) [[A]] The method according to claim 1, wherein said storage entry is selected from the group ~~comprising~~ consisting of: a file[[,]]; a registry entry[[,]]; and a database entry.

5. (Currently amended) [[A]] The method according to claim 1, wherein said identity is selected from the group ~~comprising~~ consisting of: a serial number[[,]]; a model type ~~number,~~; a component type; a volume name; a physical location[[,]]; and a network address.

6. (Currently amended) [[A]] The method according to claim 1, wherein said ~~at least one~~ computer component is selected from the group ~~comprising~~ consisting of: a hard drive[[,]]; a network card[[,]]; a CPU, a computer chip[[,]]; a ~~software element~~ computer program[[,]]; ~~a hardware element,~~ a BIOS[[,]]; and a file~~, a name of a file, an ID of a file, a physical location of a file, a program~~.

7. (Currently amended) [[A]] The method according to claim 1, wherein said deriving a name ~~of said at least one identifier from said identity of said at least one computer component is carried out by the steps~~ further comprises:

a) generating a pseudo-random sequence whose seed is based on a numeric value derived from said identity; and

b) deriving said ~~at least one identifier~~ name from at least one member of said pseudo-random sequence.

8. (Currently amended) [[A]] The method according to claim 1, wherein said ~~at least one~~ computer component is remotely accessible by said computer.

9. (Canceled)

10. (Currently amended) A method for ~~securely storing~~ hiding information on a computer and retrieving [[said]] the information, [[said]] the method comprising ~~the steps of~~:

storing [[said]] the information by:

a) retrieving an identity of ~~at least one~~ a computer component;

b) deriving ~~at least one identifier~~ a name from said identity in a secret manner ~~of said at least one computer component~~;

c) ~~for each of said at least one identifier,~~ storing [[said]] the information on [[said]] the computer in a storage entry ~~corresponding to~~ identified by said ~~identifier~~ name;

retrieving the ~~stored~~ information by:

d) retrieving [[the]] said identity of said ~~at least one~~ computer component;

e) deriving in the manner of step (b) said ~~at least one identifier~~ name from said identity ~~of at least one computer component~~ in said secret manner; and

f) ~~for each of said at least one identifier,~~ retrieving [[said]] the information ~~on said computer~~ from [[a]] said storage entry ~~corresponding to~~ identified by said ~~identifier~~ name;

11. (Canceled)

12. (Currently amended) [[A]] The method according to claim 10, wherein [[said]] the information is encrypted prior to said storing ~~of said information~~.

13. (Currently amended) [[A]] The method according to claim 10, wherein said storage entry is selected from the group ~~comprising~~ consisting of: a file[[,]]; a registry entry[[,]]; and a database entry.

14. (Currently amended) [[A]] The method according to claim 10, wherein said identity is selected from the group ~~comprising~~ consisting of: a serial number[[,]]; a model type ~~number,~~; a component type; a volume name; a physical location[[,]]; and a network address.

15. (Currently amended) [[A]] The method according to claim 10, wherein said ~~at least one~~ computer component is selected from the group ~~comprising~~ consisting of: a hard drive[[,]]; a network card[[,]]; a CPU, a computer chip[[,]]; a ~~software element~~ computer program[[,]]; ~~a hardware element,~~ a BIOS[[,]]; and a file~~, a name of a file, an ID of a file, a physical location of a file, a program~~.

16. (Currently amended) [[A]] The method according to claim 10, wherein said deriving a name ~~of said at least one identifier from said identity of said at least one computer component is carried out by the steps~~ further comprises:

a) generating a pseudo-random sequence whose seed is based on a numeric value derived from said identity; and

b) deriving said ~~at least one identifier~~ name from at least one member of said pseudo-random sequence.

17. (Currently amended) [[A]] The method according to claim 10, wherein said ~~at least one~~ computer component is remotely accessible by said computer.

18. (Canceled)

For the convenience of the Examiner, following is a clean version of the above amended claims, showing the status indicators, but without the tracking markup:

1. (Currently amended) A method for hiding information on a computer, the method comprising:

a) retrieving an identity of a computer component;

b) deriving a name from said identity in a secret manner; and

c) storing the information on the computer in a storage entry identified by said name.

2. (Canceled)

3. (Currently amended) The method according to claim 1, wherein the information is encrypted prior to said storing.

4. (Currently amended) The method according to claim 1, wherein said storage entry is selected from the group consisting of: a file; a registry entry; and a database entry.

5. (Currently amended) The method according to claim 1, wherein said identity is selected from the group consisting of: a serial number; a model type; a component type; a volume name; a physical location; and a network address.

6. (Currently amended) The method according to claim 1, wherein said computer component is selected from the group consisting of: a hard drive; a network card; a CPU, a computer chip; a computer program; a BIOS; and a file.

7. (Currently amended) The method according to claim 1, wherein said deriving a name further comprises:

a) generating a pseudo-random sequence whose seed is based on a numeric value derived from said identity; and

b) deriving said name from at least one member of said pseudo-random sequence.

8. (Currently amended) The method according to claim 1, wherein said computer component is remotely accessible by said computer.

9. (Canceled)

10. (Currently amended) A method for hiding information on a computer and retrieving the information, the method comprising:

storing the information by:

a) retrieving an identity of a computer component;

b) deriving a name from said identity in a secret manner;

c) storing the information on the computer in a storage entry identified by said name;

retrieving the information by:

d) retrieving said identity of said computer component;

e) deriving in the manner of step (b) said name from said identity in said secret manner; and

f) retrieving the information from said storage entry identified by said name;

11. (Canceled)

12. (Currently amended) The method according to claim 10, wherein the information is encrypted prior to said storing.

13. (Currently amended) The method according to claim 10, wherein said storage entry is selected from the group consisting of: a file; a registry entry; and a database entry.

14. (Currently amended) The method according to claim 10, wherein said identity is selected from the group consisting of: a serial number; a model type; a component type; a volume name; a physical location; and a network address.

15. (Currently amended) The method according to claim 10, wherein said computer component is selected from the group consisting of: a hard drive; a network card; a CPU, a computer chip; a computer program; a BIOS; and a file.

16. (Currently amended) The method according to claim 10, wherein said deriving a name further comprises:

a) generating a pseudo-random sequence whose seed is based on a numeric value derived from said identity; and

b) deriving said name from at least one member of said pseudo-random sequence.

17. (Currently amended) The method according to claim 10, wherein said computer component is remotely accessible by said computer.

18. (Canceled)